Radiator

Sistema Operativo	CentOS 6.4 i386
Nível de dificuldade	Médio
Nível de maturidade	Médio

- Créditos
- Introdução
- Obter todo o material necessário
  - Fazer o download do repositório RPMForge
  - Fazer o download do OSC Radiator
- Instalação
- Abrir os portos na firewall
- Configuração do Radiator
  - Configurações iniciais
  - Configuração dos clientes

Créditos

Este documento, que descreve em detalhe o processo de instalação e configuração do servidor de RADIUS Radiator com autenticação em LDAP para a rede eduroam, foi escrito e disponibilizado pelos Serviços de Informática do Instituto Politécnico de Castelo Branco.

Grande parte das configurações foram discutidas com os técnicos da FCCN, nomeadamente o Pedro Simões, pelo que aqui fica o nosso agradecimento pelo tempo e paciência despendidos.

Introdução

O Radiator é um servidor RADIUS comercial produzido pela OSC - Open System Consultants (http://www.open.com.au/) que tem a particularidade de ser extremamente versátil e configurável.

Neste documento são descritos os seguintes procedimentos:

- Instalação do Radiator;
- Configuração do Radiator para a eduroam com autenticação LDAP;
- Envio de informações sobre autenticações via syslog para a FCCN;

Obter todo o material necessário

Fazer o download do repositório RPMForge

```
wget http://pkgs.repoforge.org/rpmforge-release/rpmforge-release-0.5.3-1.el6.rf.i686.rpm
```

Para mais informações sobre outras plataformas consultar http://repoforge.org/use/

Fazer o download do OSC Radiator

1. Aceder a http://www.open.com.au/radiator/downloads.HTML;
2. Seleccionar “Full Licensed customers” e introduzir as credenciais de acesso;
3. Fazer o download da versão “RPM format for Linux”;

Instalação

Instalar o RPMForge para podermos instalar facilmente os restantes pacotes:

```
rpm -i rpmforge-release-0.5.3-1.el6.rf.i686.rpm
```

Instalar os pacotes necessários ao funcionamento do Radiator:

```
yum install perl-DBI
yum install perl-DBD-mysql
yum install perl-Digest-MD4
yum install perl-LDAP
yum install perl-Tk
```

O Radiator necessita ainda destes dos pacotes:

- perl-Digest-MD5 - vem instalado de raiz;
- perl-Digest-SHA1 - é uma dependência do pacote perl-LDAP pelo que é instalado quando este;
- perl-Digest-HMAC - é uma dependência do pacote perl-LDAP pelo que é instalado quando este;

Instalar o Radiator:

```
rpm -ivh Radiator-4.9-2.noarch.rpm
```

Abrir os portos na firewall

Existem várias formas de executar este passo, executando o comando setup é uma delas ou então da forma descrita:

Editar os ficheiros /etc/sysconfig/iptables e /etc/sysconfig/ip6tables e acrescentar as linhas necessária a abrir os portos UDP 1812, 1813, 1645 e 1646:

```
-A INPUT -m state --state NEW -m udp -p udp --dport 1812 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 1813 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 1645 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 1646 -j ACCEPT
```

Exemplo /etc/sysconfig/iptables:

```
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 1812 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 1813 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 1645 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 1646 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

Exemplo /etc/sysconfig/ip6tables:

```
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p ipv6-icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 1812 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 1813 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 1645 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 1646 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp6-adm-prohibited
-A FORWARD -j REJECT --reject-with icmp6-adm-prohibited
COMMIT
```

Finalmente reiniciar os serviços iptables e ip6tables:

```
service iptables restart
service ip6tables restart
```

Configuração do Radiator

Configurações iniciais

1. Diretoria de logs:

logs

```
LogDir        /var/log/radius
```

2. Diretoria de base de dados de utilizadores em ficheiro e dicionário:

Db

```
DbDir        /etc/radiator
```

3. Ficheiro de dicionário:

dicionário

```
DictionaryFile        %D/dictionary.dat
```

4. Nível de detalhe dos logs:

trace

```
# 0 ERR. Error conditions. Serious and unexpected failures
# 1 WARNING. Warning conditions. Unexpected failures
# 2 NOTICE. Normal but significant conditions.
# 3 INFO. Informational messages.
# 4 DEBUG. Debugging messages.
# 5 EXTRA_DEBUG. Incoming raw packet dumps in hexadecimal

Trace        0
```

5. Configurações de rede:

rede

```
BindAddress        ipv6:2001:690:2260:101::99, 10.10.0.99
AuthPort        1812,1645
AcctPort        1813,1646
```

Configuração dos clientes

Por clientes entendem-se AP's, Controladoras de AP's, Servidores de VPN, Radius Nacional FCCN e etc. que farão pedidos de autenticação e accounting ao Radiator.

Apesar de poderem ser configurados no ficheiro principal a melhor opção é separar em ficheiros de forma a ser mais fácil a sua configuração.

- Ficheiro /etc/radiator/nas/aps.cfg:

aps.cfg

```
# AP'S DO EDIFICIO 1
<Client 10.241.0.1>
        Secret <ALTERAR PARA UM BOM SEGREDO>
        IdenticalClients 10.241.0.2 10.241.0.3 <ACRESCENTAR OS IP'S DOS CLIENTES COM A MESMA
CONFIGURAÇÃO>
        Identifier AP-SITE1
        StripFromReply Vendor-Specific
</Client>

# AP'S DO EDIFICIO 2
<Client 10.242.0.1>
        Secret <ALTERAR PARA UM BOM SEGREDO>
        IdenticalClients 10.242.0.2 10.242.0.3 <ACRESCENTAR OS IP'S DOS CLIENTES COM A MESMA
CONFIGURAÇÃO>
        Identifier AP-SITE2
        StripFromReply Vendor-Specific
</Client>
```

- Ficheiro /etc/radiator/nas/fccn.cfg:

fccn.cfg

```
# PROXY NACIONAL
# PEDIDOS DE AUTENTICAÇÃO DE UTILIZADORES NOSSOS EM OUTRAS INSTITUIÇÕES
<Client ipv6:2001:690:a00:4001::43>
        Identifier 4ProxyServer
        IdenticalClients ipv6:2001:690:a00:4001::44, 193.136.192.43, 193.136.192.44, cv-radius.fccn.pt,
cv2-radius.fccn.pt
        Secret <FALEM COM O PEDRO SIMÕES>
        StripFromReply Vendor-Specific,Class,Tunnel-Type,Tunnel-Medium-Type,Tunnel-Private-Group-ID,
Filter-Id,Cisco-AVPair
        NoIgnoreDuplicates Accounting-Request
</Client>
```

- Podem-se acrescentar tantos ficheiros quantos necessários para que a configuração fique fácil de alterar.

Configuração do cliente: Proxy Nacional

A utilização da opção **StripFromReply** prende-se com o facto de que não devemos enviar atributos destinados aos nossos clientes locais (AP's, VPN's etc.) com configurações locais sob pena de estarmos a interferir nas configurações locais da instituição remota (ex. um utilizador apesar de autenticar corretamente não consegue aceder à rede por estar numa VLAN que não existe onde ele se encontra, mas que existe na instituição de origem).

Atributos que devem sempre ser removidos independentemente da configuração:

- Tunnel-Type, Tunnel-Medium-Type e Tunnel-Private-Group-ID;
- Filter-Id;
- Cisco-AVPair;
- Vendor-Specific;
- Atributos específicos da vossa configuração (No nosso caso o Class);

Após a configuração destes ficheiros é necessário acrescentar um entrada no ficheiro principal (/etc/radiator/radius.cfg) de forma a que o Radiator os inclua quando executado:

radius.cfg - clientes

```
include %D/nas/aps.cfg
include %D/nas/fccn.cfg
```